CLAIMS:

1. A data processing device, in particular an electronic memory component, comprising a plurality of access-secured sub-areas, in particular a plurality of access-secured memory areas, each having at least one assigned parameter (a_n, a_{n-1},..., a_1, a_0), in particular address, characterized in that the parameter (a_n, a_{n-1},..., a_1, a_0) of at least one sub-area may be encrypted only in certain areas, i.e. in dependence on at least one further sub-area (a'_n, a'_{n-1},..., a'_1, a'_0).

2. A data processing device as claimed in claim 1, characterized in that the parameter to be encrypted (a_n, a_{n-1},..., a_1, a_0) may be encrypted in dependence, in particular as function ($f_1(a_n)$, $f_2(f_1(a_n),a_{n-1})$,..., $f_n(f_{n-1}(...))$, $f_{n+1}(f_n(f_{n-1}(...)))$), on at least one parameter of the further sub-area (a'_n, a'_{n-1},..., a'_1, a'_0).

3. A data processing device as claimed in claim 2, characterized in that
- the input value (a_n, a_{n-1},..., a_1, a_0) to the function (f_i) and/or
- the return value (a'_n, a'_{n-1},..., a'_1, a'_0) from the function (f_i)

is more than one bit wide.

4. A data processing device as claimed in at least one of claims 1 to 3, characterized in that the memory component takes the form of
- an E[rasable]P[rogrammable]R[ead] O[nly]M[emory],
- an E[lectrically]E[rasable]P[rogrammable]R[ead]O[nly]M[emory] or
- a Flash memory.

5. A microcontroller, in particular a smart card controller, comprising at least one data processing device as claimed in at least one of claims 1 to 4.

6. A method of encrypting at least one parameter (a_n, a_{n-1},..., a_1, a_0), in particular the address, of at least one access-secured sub-area, in particular at least one access-secured memory area, of at least one data processing device, in particular at least one electronic

memory component characterized in that the parameter to be encrypted (a_n, a_{n-1},..., a_1, a_0) of the sub-area is encrypted only in certain areas, i.e. in dependence on at least one further sub-area (a'_n, a'_{n-1},..., a'_1, a'_0).

7. A method as claimed in claim 6, characterized in that the parameter to be encrypted (a_n, a_{n-1},..., a_1, a_0) of the sub-area is encrypted in dependence, in particular as function ($f_1(a_n)$, $f_2(f_1(a_n),a_{n-1})$,..., $f_n(f_{n-1}(...))$, $f_{n+1}(f_n(f_{n-1}(...)))$), on at least one parameter of the further sub-area (a'_n, a'_{n-1},..., a'_1, a'_0).

8. A method as claimed in claim 7, characterized in that the function $f_i(a)$ is one-to-one.

9. A method as claimed in at least one of claims 6 to 8, characterized in that the access-secured sub-areas, in particular the access-secured memory areas, are secured separately.

10. Use of at least one data processing device, in particular at least one electronic memory component,. as claimed in at least one of claims 1 to 4 in at least one chip unit, in particular

- in at least one smart card controller,
- in at least one reader I[ntegrated] C[ircuit] or
- in at least one crypto chipset,

for example in the field of audio and/or video encryption.